

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004年4月1日 (01.04.2004)

PCT

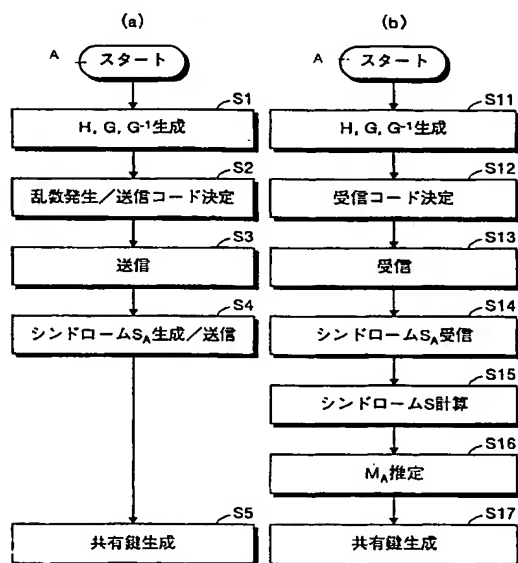
(10) 国際公開番号
WO 2004/028074 A1

- (51) 国際特許分類: H04L 9/12, H03M 13/09, H04B 10/00
- (21) 国際出願番号: PCT/JP2003/011706
- (22) 国際出願日: 2003年9月12日 (12.09.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-271473 2002年9月18日 (18.09.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP). 理化学研究所 (RIKEN) [JP/JP]; 〒351-0198 埼玉県和光市広沢2番1号 Saitama (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 松本 渉 (MATSUMOTO, Wataru) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP). 渡辺 曜大 (WATANABE, Youdai) [JP/JP]; 〒351-0198 埼玉県和光市広沢2番1号 理化学研究所内 Saitama (JP).
- (74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒100-0013 東京都千代田区霞が関三丁目2番6号 東京倶楽部ビルディング Tokyo (JP).
- (81) 指定国 (国内): AU, CA, CN, KR, NO, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

[続葉有]

(54) Title: QUANTUM KEY DISTRIBUTION METHOD AND COMMUNICATION DEVICE

(54) 発明の名称: 量子鍵配送方法および通信装置



A...START
 S1...H, G, G⁻¹ GENERATION
 S2...RANDOM NUMBER GENERATION/TRANSMISSION CODE
 DECISION
 S3...TRANSMISSION
 S4...SYNDROME S_A GENERATION/TRANSMISSION
 S5...SHARED KEY GENERATION
 S11...H, G, G⁻¹ GENERATION
 S12...RECEPTION CODE DECISION
 S13...RECEPTION
 S14...SYNDROME S_A RECEPTION
 S15...SYNDROME S CALCULATION
 S16...M_A ESTIMATION
 S17...SHARED KEY GENERATION

(57) Abstract: It is possible to create a shared key whose safety is surely guaranteed while correcting a data error in the transmission path by using an error correction code having an extremely high characteristic. According to a quantum key distribution method, firstly, a communication device of the reception side corrects the data error of the reception data by using a parity inspection matrix for an "Irregular-LDPC code" which is determinate and has stable characteristic. The communication device of the reception side and the communication device of the transmission side discard a part of shared information according to the error correction information disclosed.

(57) 要約: 極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成するため、本発明の量子鍵配送方法では、まず、受信側の通信装置が、確定的で特性が安定した「Irregular-LDPC符号」用のパリティ検査行列を用いて受信データのデータ誤りを訂正する。そして、受信側の通信装置および送信側の通信装置が、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。



添付公開書類:

— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

量子鍵配送方法および通信装置

5 技術分野

本発明は、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法に関するものであり、特に、誤り訂正符号を用いてデータ誤りを訂正可能な量子鍵配送方法および当該量子鍵配送を実現可能な通信装置に関するものである。

10

背景技術

以下、従来の量子暗号システムについて説明する。近年、高速大容量な通信技術として光通信が広く利用されているが、このような光通信システムでは、光のオン／オフで通信が行われ、オンのときに大量の光子が送信されているため、量子効果が直接現れる通信系にはなっていない。

15

一方、量子暗号システムでは、通信媒体として光子を用い、不確定性原理等の量子効果が生じるように1個の光子で1ビットの情報を伝送する。このとき、盗聴者が、その偏光、位相等の量子状態を知らずに適当に基底を選んで光子を測定すると、その量子状態に変化が生じる。したがって、受信側では、この光子の量子状態の変化を確認することによって、伝送データが盗聴されたかどうかを認識することができる。

20

第9図は、従来の偏光を利用した量子鍵配送の概要を示す図である。たとえば、水平垂直方向の偏光を識別可能な測定器では、量子通信路上の、水平方向（0°）に偏光された光と垂直方向（90°）に偏光された光とを正しく識別する。一方、斜め方向（45°，135°）の偏光を識別可能な測定器では、量子通信路上の、45°方向に偏光された光と135°方向に偏光された光とを正しくを識別する。

25

このように、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（ 0° ， 90° ）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ50%の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

第9図に示す従来の量子鍵配送では、上記不確定性（ランダム性）を利用して、盗聴者に知られずに送信者と受信者との間で鍵を共有する（たとえば、非特許文献1参照。）。なお、送信者および受信者は、量子通信路以外に公開通信路を使用することができる。ここで、鍵の共有手順について説明する。

まず、送信者は、乱数列（1，0の列：送信データ）を発生し、さらに送信コード（+：水平垂直方向に偏光された光を識別可能な測定器に対応，×：斜め方向に偏光された光を識別可能な測定器に対応）をランダムに決定する。その乱数列と送信コードの組み合わせで、送信する光の偏光方向が自動的にきまる。ここでは、0と+の組み合わせで水平方向に偏光された光を、1と+の組み合わせで垂直方向に偏光された光を、0と×の組み合わせで 45° 方向に偏光された光を、1と×の組み合わせで 135° 方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

つぎに、受信者は、受信コード（+：水平垂直方向に偏光された光を識別可能な測定器，×：斜め方向に偏光された光を識別可能な測定器）をランダムに決定し、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって受信データを得る。ここでは、受信データとして、水平方向に偏光された光と+の組み合わせで0を、垂直方向に偏光された光と+の組み合わせで1を、 45° 方向に偏光された光と×の組み合わせで0を、 135° 方向に偏光された光と×の組み合わせで0を、それぞれ得る。

つぎに、受信者は、自身の測定が正しい測定器で行われたものかどうかを調べるために、受信コードを、公開通信路を介して送信者に対して送信する。受信コ

ードを受け取った送信者は、正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信者に対して返信する。

つぎに、受信者は、正しい測定器で受信した受信信号に対応する受信データだけを残し、その他を捨てる。この時点で、残された受信データは送信者と受信者
5 との間で確実に共有できている。

つぎに、送信者と受信者は、それぞれの通信相手に対して、共有データから選択した所定数のデータを、公開通信路を経由して送信する。そして、受け取ったデータが自信の持つデータと一致しているかどうかを確認する。たとえば、確認したデータの中に一致しないデータが1つでもあれば、盗聴者がいるものと判断
10 して共有データを捨て、再度、鍵の共有手順を最初からやり直す。一方、確認したデータがすべて一致した場合には、盗聴者がいないと判断し、確認に使用したデータを捨て、残った共有データを送信者と受信者の共有鍵とする。

また、上記従来の量子鍵配送方法の応用として、たとえば、伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法がある（たとえば、非特許文献2参照。
15 ）。

この方法では、送信者が、データ誤りを検出するために、送信データを複数のブロックに分割し、ブロック毎のパリティを公開通信路上に送信する。そして、受信者が、公開通信路を経由して受け取ったブロック毎のパリティと受信データにおける対応するブロックのパリティとを比較して、データ誤りをチェックする。
20 このとき、異なるパリティがあった場合、受信者は、どのブロックのパリティが異なっているのかを示す情報を公開通信路上に返信する。そして、送信者は、該当するブロックをさらに前半部のブロックと後半部のブロックに分割し、たとえば、前半部のパリティを公開通信路上に返信する（二分探索）。以降、送信者と受信者は、上記二分探索を繰り返し実行することによりエラービットの位置を特定し、最終的に受信者がそのビットを訂正する。
25

さらに、送信者は、データに誤りがあるにもかかわらず、偶数個の誤りのために正しいと判定されたパリティがある場合を想定し、送信データをランダムに並

べ替えて（ランダム置換）複数のブロックに分割し、再度、上記二分探索による誤り訂正処理を行う。そして、ランダム置換によるこの誤り訂正処理を繰り返し実行することによって、すべてのデータ誤りを訂正する。

非特許文献 1.

- 5 Bennett, C. H. and Brassard, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing, In Proceedings of IEEE Conference on Computers, System and Signal Processing, Bangalore, India, pp.175-179 (DEC.1984).

非特許文献 2.

- 10 Brassard, G. and Salvail, L. 1993 Secret-Key Reconciliation by Public Discussion, In Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765, 410-423.

しかしながら、上記第 9 図に示す従来の量子鍵配送においては、誤り通信路を想定していないため、誤りがある場合には盗聴行為が存在したものと
15 して上記共通データ（共通鍵）を捨てることとなり、伝送路によっては共通鍵の生成効率が非常に悪くなる、という問題があった。

また、上記伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法においては、エラービットを特定するために膨大な回数のパリティのやりとりが発生し、さらに、ランダム置換による誤り訂正処理が所定回数にわたって行われるため、
20 誤り訂正処理に多大な時間を費やすことになる、という問題があった。

従って、本発明は、極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法を提供することを目的としている。

25 発明の開示

本発明にかかる量子鍵配送方法にあつては、光子を量子通信路上に送信する第 1 の通信装置と当該光子を測定する第 2 の通信装置で構成された量子暗号システ

- ムにて実行され、たとえば、前記第1および第2の通信装置が、同一のパリティ検査行列 H ($n \times k$) を生成する検査行列生成ステップと、前記第1の通信装置が、乱数列(送信データ)を発生し、さらに所定の送信コード(基底)をランダムに決定し、前記第2の通信装置が、所定の受信コード(基底)をランダムに決定する乱数発生ステップと、前記第1の通信装置が、前記送信データと送信コードの組み合わせによって規定された量子状態で、光子を量子通信路上に送信する光子送信ステップと、前記第2の通信装置が、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを得る光子受信ステップと、前記第1および第2の通信装置が、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定された n ビットの受信データおよび対応する送信データを残し、その他を捨てるデータ削除ステップと、前記第1の通信装置が、前記パリティ検査行列 H と n ビットの送信データに基づく k ビットの誤り訂正情報を、公開通信路を介して前記第2の通信装置に通知する誤り訂正情報通知ステップと、前記第2の通信装置が、前記パリティ検査行列 H と n ビットの受信データと誤り訂正情報に基づいて、受信データの誤りを訂正する誤り訂正ステップと、前記第1および第2の通信装置が、公開された誤り訂正情報に応じて誤り訂正後の共有情報(n)の一部(k)を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を装置間の共有鍵とする暗号鍵生成ステップと、を含むことを特徴とする。
- 20 この発明によれば、確定的で特性が安定した「Irregular-LDPC符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、さらに、公開された誤り訂正情報に応じて共有情報の一部を捨てる。

図面の簡単な説明

- 25 第1図は、本発明にかかる量子暗号システムの実施の形態1の構成を示す図であり、第2図は、実施の形態1の量子鍵配送を示すフローチャートであり、第3図は、有限アフィン幾何に基づく「Irregular-LDPC符号」の構成

法を示すフローチャートであり、第4図は、有限アフィン幾何符号 $AG(2, 2^2)$ のマトリクスを示す図であり、第5図は、最終的な列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_j を示す図であり、第6図は、ランダム系列のラテン方阵行列による分割手順を示す図であり、第7図は、本発明にかかる量子暗号システムの実施の形態2の構成を示す図であり、第8図は、実施の形態2の量子鍵配送を示すフローチャートであり、第9図は、従来の量子鍵配送の概要を示す図である。

発明を実施するための最良の形態

以下に、本発明にかかる量子鍵配送方法の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。また、以下では、例として偏光を利用する量子鍵配送について説明するが、本発明は、たとえば、位相を利用するもの、周波数を利用するもの等にも適用可能であり、どのような量子状態を利用するかについては特に限定しない。

実施の形態1.

量子鍵配送は、盗聴者の計算能力によらず、安全性の保証された鍵配送方式であるが、たとえば、より効率よく共有鍵を生成するためには、伝送路を通ることによって発生するデータの誤りを取り除く必要がある。そこで、本実施の形態では、極めて高い特性をもつことが知られている低密度パリティ検査 (LDPC : Low-Density Parity-Check) 符号を用いて誤り訂正を行う量子鍵配送について説明する。

第1図は、本発明にかかる量子暗号システムにおける通信装置 (送信機, 受信機) の構成を示す図である。この量子暗号システムは、情報 m_s を送信する機能を備えた送信側の通信装置と、伝送路上で雑音等の影響を受けた情報 m_r 、すなわち情報 m_s を受信する機能を備えた受信側の通信装置と、から構成される。

また、送信側の通信装置は、量子通信路を介して情報 m_s を送信し、公開通信路を介してシンδροーム s_A を送信し、これらの送信情報に基づいて暗号鍵 (受信側との共通鍵) を生成する暗号鍵生成部1と、暗号化部2が暗号鍵に基づい

て暗号化したデータを、送受信部 2 2 が公開通信路を介してやりとりする通信部 2 と、を備え、受信側の通信装置は、量子通信路を介して情報 m_b を受信し、公開通信路を介してシンドローム s_A を受信し、これらの受信情報に基づいて暗号鍵（送信側との共通鍵）を生成する暗号鍵生成部 3 と、暗号化部 4 2 が暗号鍵に基づいて暗号化したデータを、送受信部 4 1 が公開通信路を介してやりとりする通信部 4 と、を備える。

上記送信側の通信装置では、量子通信路上に送信する情報 m_a として、偏光フィルターを用いて所定の方に偏光させた光（第 9 図参照）を、受信側の通信装置に対して送信する。一方、受信側の通信装置では、水平垂直方向（ 0° , 90° ）の偏光を識別可能な測定器と斜め方向（ 45° , 135° ）の偏光を識別可能な測定器とを用いて、量子通信路上の、水平方向（ 0° ）に偏光された光と垂直方向（ 90° ）に偏光された光と 45° 方向に偏光された光と 135° 方向に偏光された光とを識別する。なお、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（ 0° , 90° ）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ 50% の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

以下、上記量子暗号システムにおける各通信装置の動作、すなわち、本実施の形態における量子鍵配送について詳細に説明する。第 2 図は、本実施の形態の量子鍵配送を示すフローチャートであり、詳細には、（a）は送信側の通信装置の処理を示し、（b）は受信側の通信装置の処理を示す。

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部 10 , 30 が、特定の線形符号のパリティ検査行列 H ($n \times k$) を求め、このパリティ検査行列 H から「 $HG = 0$ 」を満たす生成行列 G ($(n - k) \times n$) を求め、さらに、 $G^{-1} \cdot G = I$ （単位行列）となる G の逆行列 G^{-1} ($n \times (n - k)$) を求める（ステップ S 1 , ステップ S 11）。本実施の形態では、上記

特定の線形符号として、シャノン限界に極めて近い優れた特性をもつLDPC符号を用いた場合の量子鍵配送について説明する。なお、本実施の形態では、誤り訂正方式としてLDPC符号を用いることとしたが、これに限らず、たとえば、ターボ符号等の他の線形符号を用いることとしてもよい。また、たとえば、後述する誤り訂正情報（シンドローム）が適当な行列 H と情報 m_A の積 Hm_A で表される誤り訂正プロトコル（たとえば、従来技術にて説明した「伝送路上におけるデータ誤りを訂正可能な量子鍵配送」に相当する誤り訂正プロトコル）であれば、すなわち、誤り訂正情報と情報 m_A の線形性が確保されるのであれば、その行列 H を用いることとしてもよい。

- 10 ここで、上記パリティ検査行列生成部10におけるLDPC符号の構成法について、詳細には、有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法（第2図ステップS1の詳細）について説明する。第3図は、有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法を示すフローチャートである。なお、パリティ検査行列生成部30については、パリティ検査行列生成部10と同様に動作するのでその説明を省略する。また、本実施の形態における検査行列生成処理は、たとえば、設定されるパラメータに応じてパリティ検査行列生成部10で実行する構成としてもよいし、通信装置外部の他の制御装置（計算機等）で実行することとしてもよい。本実施の形態における検査行列生成処理が通信装置外部で実行される場合は、生成済みの検査行列が通信装置に格納される。以降の実施の形態では、パリティ検査行列生成部10で上記処理を実行する場合について説明する。

- 25 まず、パリティ検査行列生成部10では、「Irregular-LDPC符号」用の検査行列のベースとなる有限アフィン幾何符号 $AG(2, 2^s)$ を選択する（第3図、ステップS21）。ここでは、行の重みと列の重みがそれぞれ 2^s となる。第4図は、たとえば、有限アフィン幾何符号 $AG(2, 2^2)$ のマトリクスを示す図（空白は0を表す）である。

つぎに、パリティ検査行列生成部10では、列の重みの最大値 r_1 （ $2 < r_1 \leq$

2^s) を決定する (ステップ S 2 2)。そして、符号化率 *rate* (1 - シンドローム長 / 鍵の長さ) を決定する (ステップ S 2 2)。

つぎに、パリティ検査行列生成部 10 では、ガウス近似法 (Gaussian Approximation) による最適化を用いて、暫定的に、列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_u を求める (ステップ S 2 3)。なお、行の重み配分の生成関数 $\rho(x)$ は $\rho(x) = \rho_u x^{u-1} + (1 - \rho_u) x^u$ とする。また、重み u は $u \geq 2$ の整数であり、 ρ_u は行における重み u の割合を表す。

つぎに、パリティ検査行列生成部 10 では、有限アフィン幾何の行の分割により構成可能な、行の重み $\{u, u+1\}$ を選択し、さらに (1) 式を満たす分割係数 $\{b_u, b_{u+1}\}$ を求める (ステップ S 2 4)。なお、 b_u, b_{u+1} は非負の整数とする。

$$b_u + b_{u+1}(u+1) = 2^s \quad \dots (1)$$

具体的には、下記 (2) 式から b_u を求め、上記 (1) 式から b_{u+1} を求める。

$$\arg \min_{b_u} \left| \varphi_u - \frac{u \times b_u}{2^s} \right| \quad \dots (2)$$

つぎに、パリティ検査行列生成部 10 では、上記決定したパラメータ $u, u+1, b_u, b_{u+1}$ によって (上記行の分割処理によって) 更新された行の重みの比率 ρ'_u, ρ'_{u+1} を (3) 式により求める (ステップ S 2 5)。

$$\begin{aligned} \varphi'_u &= \frac{u \times b_u}{2^s} \\ \varphi'_{u+1} &= \frac{(u+1) \times b_{u+1}}{2^s} \end{aligned} \quad \dots (3)$$

つぎに、パリティ検査行列生成部 10 では、ガウス近似法による最適化を用いて、さらに上記で求めた $u, u+1, \rho'_u, \rho'_{u+1}$ を固定のパラメータとして、

暫定的に、列の重み配分 $\lambda(\gamma_i)$ を求める (ステップ S 2 6)。なお、重み γ_i は $\gamma_i \geq 2$ の整数であり、 $\lambda(\gamma_i)$ は列における重み γ_i の割合を表す。また、列数が 1 以下となる重み ($\lambda(\gamma_i) \leq \gamma_i / w_t$, i は正の整数) を候補から削除する。ただし、 w_t は AG (2, 2^s) に含まれる 1 の総数を表す。

- 5 つぎに、上記で求めた重み配分を満たし、かつ下記 (4) 式を満たす、列の重み候補のセット $\{\gamma_1, \gamma_2, \dots, \gamma_l (\gamma_l \leq 2^s)\}$ を選択する (ステップ S 2 7)。そして、下記の (4) 式を満たさない列の重み γ_i が存在する場合には、その列の重みを候補から削除する。

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,l} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,l} \\ \vdots & & \cdots & \vdots \end{bmatrix} \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_l \end{bmatrix} = \begin{bmatrix} 2^s \\ 2^s \\ \vdots \\ 2^s \end{bmatrix} \quad \cdot \cdot \cdot \quad (4)$$

- 10 なお、各 a は、列の重み 2^s を構成するための $\{\gamma_1, \gamma_2, \dots, \gamma_l\}$ に対する非負の整数となる係数を表し、 i, j は正の整数であり、 γ_i は列の重みを表し、 γ_l は列の最大重みを表す。

- つぎに、パリティ検査行列生成部 10 では、ガウス近似法による最適化を用いて、さらに上記で求めた $u, u+1, \rho_u, \rho_{u+1}$ と $\{\gamma_1, \gamma_2, \dots, \gamma_l\}$ を固定
15 パラメータとして、列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_u を求める (ステップ S 2 8)。

- つぎに、パリティ検査行列生成部 10 では、分割処理を行う前に、列の重み配
分 $\lambda(\gamma_i)$ と行の重み配分 ρ_u を調整する (ステップ S 2 9)。なお、調整後
の各重みの配分は、可能な限りガウス近似法で求めた値に近い値にする。第 5 図
20 は、ステップ S 2 9 における最終的な列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_u を示す図である。

最後に、パリティ検査行列生成部 10 では、有限アフィン幾何における行および列を分割して (ステップ S 3 0)、 $n \times k$ のパリティ検査行列 H を生成する。

本発明における有限アフィン幾何符号の分割処理は、規則的に分割するのではなく、各行または各列から「1」の番号をランダムに抽出する（後述するランダム分割の具体例を参照）。なお、この抽出処理は、ランダム性が保持されるのであればどのような方法を用いてもよい。

5 具体的にいうと、EG (2, 2⁵) における1列中の「1」の行番号が、
 $B_1(x) = \{1 \ 32 \ 114 \ 136 \ 149 \ 223 \ 260 \ 382 \ 402 \ 438 \ 467 \ 507 \ 574 \ 579 \ 588 \ 622$
 $634 \ 637 \ 638 \ 676 \ 717 \ 728 \ 790 \ 851 \ 861 \ 879 \ 947 \ 954 \ 971 \ 977 \ 979 \ 998\}$

の場合、分割後の行列における1～4列目 $R_n(n)$ は、 $B_1(x)$ から「1」の番号がランダムに抽出され、たとえば、

10 $R_1(n) = \{1 \ 114 \ 574 \ 637 \ 851 \ 879 \ 977 \ 979\}$
 $R_2(n) = \{32 \ 136 \ 402 \ 467 \ 588 \ 728 \ 861 \ 971\}$
 $R_3(n) = \{149 \ 260 \ 382 \ 438 \ 579 \ 638 \ 717 \ 998\}$
 $R_4(n) = \{223 \ 507 \ 622 \ 634 \ 676 \ 790 \ 947 \ 954\}$
 となる。

15 ここで、上記ランダム分割の一例、すなわち、上記「乱数系列のラテン方陣を用いた分割方法」を詳細に説明する。ここでは、ランダム分割を行う場合のランダム系列を容易かつ確定的に生成する。この方法による利点は、送信側と受信側が同じランダム系列を生成できることにある。

(1) 基本のランダム系列を作成する。ここでは、有限アフィン幾何AG (2, 2^s) を用い、Pを $P \geq 2^s$ を満たす最小の素数とした場合の、基本のランダム系列C (i) を (5) 式にしたがって作成する。

$$C(1) = 1$$

$$C(i+1) = G_0 \times C(i) \mod P \quad \dots (5)$$

20 なお、 $i = 0, 1, \dots, P-2$ とし、 G_0 はガロア体GF (P) の原始元である。また、系列長が2^sとなるように、2^sより大きい数をC (i) の中から削除し、削除後のC (i) を基本のランダム系列とする。

(2) 基本のランダム系列C (i) を一定間隔で読み出すためにスキップ間隔S

(j) を以下の (6) 式のように定義する。

$$S(j) = j \quad j = 1, 2, \dots, 2^s \quad \dots (6)$$

(3) 以下の (7) 式で置換パターン $LB_j(i)$ を作成する。

$$LB_j(i) = ((S(j) \times i) \bmod P) + 1$$

$$j = 1, 2, \dots, 2^s$$

$$i = 1, 2, \dots, P-1 \quad \dots (7)$$

なお、 $LB_j(i)$ も 2^s より大きい数字は削除する。

(4) q 列 i 行で j 番目のラテン方陣行列 $L_{jq}(i)$ を以下の (8) 式で算出する。

$$L_{jq}(i) = LB_j((q + i - 2) \bmod 2^s + 1)$$

$$j = 1, 2, \dots, 2^s$$

$$i = 1, 2, \dots, 2^s$$

$$q = 1, 2, \dots, 2^s \quad \dots (8)$$

(5) ラテン方陣行列 $L_{jq}(i)$ にしたがって列と行を分割する。列の分割では、

g_0, g_0, \dots, g_{n-1} をパリティ検査行列 H の列ベクトルとし、 $g_c'(k)$ を g_c , $c = 0, 1, \dots, n-1$ の列の中の k 番目の「1」とする。また、 g_c の中の「1」の位置の集合を G_c とする ((9) 式参照)。

$$G_c = \{g_c'(k), k = 1, 2, \dots, 2^s\} \quad \dots (9)$$

たとえば、 $AG(2, 2^3)$ の $c = 1$ 番目の列の「1」の行番号は、 $G_1 = \{1, 3, 8, 20, 23, 24, 34, 58\}$ となる。そして、この c 列目の列ベクトルを $g_c'(k)$ で

表現すると、(10) 式のように表すことができる。

$$g_c'(1) = ((c-1) + 1) \bmod (2^{2s} - 1)$$

$$g_c'(2) = (g_c'(1) + 2) \bmod (2^{2s} - 1)$$

$$g_c'(3) = (g_c'(2) + 5) \bmod (2^{2s} - 1)$$

$$g_c'(4) = (g_c'(3) + 12) \bmod (2^{2s} - 1)$$

$$g_c'(5) = (g_c'(4) + 3) \bmod (2^{2s} - 1)$$

$$g_c'(6) = (g_c'(5) + 1) \bmod (2^{2s} - 1)$$

$$g_{c,e}'(7) = (g_{c,e}'(6) + 10) \bmod (2^{2s} - 1)$$

$$g_{c,e}'(8) = (g_{c,e}'(7) + 24) \bmod (2^{2s} - 1) \quad \dots (10)$$

ここで、パリティ検査行列Hの各列 g_c を、上記(4)式を満たす列の次数と係数に基づいて、新しい列 $g_{c,e}$ に分割する。そして、 $g_{c,e}'(r)$ を新しい列 $g_{c,e}$ の中の r 行目の「1」とする。また、 $g_{c,e}$ の中の「1」の位置の集合を $G_{c,e}$ とする((11)式参照)。

$$G_{c,e} = \{g_{c,e}'(r), r = 1, 2, \dots\} \quad \dots (11)$$

そして、ラテン方陣行列群を用いて、下記(12)式にしたがって分割するエッジの選択を行う。なお、 $a_{t,1}, a_{t,2}, \dots, a_{t,t}$ と $\gamma_1, \gamma_2, \dots, \gamma_t$ は、上記式(4)を満たす係数と次数である。また、 t は(4)式の係数行列の行番号を示している。また、 t 行目の式で分割する有限アフィン平面の列数を n_t とし、係数行列の行番号の最大値を t_m とすると、 t は(13)式で表すことができる。

$$g'_{c,e}(r) = g'_c(L_{j,q}(i))$$

$$j = c/2^s$$

$$q = ((c-1) \bmod 2^s) + 1 \quad \dots (12)$$

$$i = r + \sum_{m=1}^{\ell} \min(a_{t,m}, \max(0, e-1 - \sum_{n=1}^{m-1} a_{t,n})) \cdot \gamma_m$$

15

$$t \begin{cases} 1(1 \leq c \leq n_1) \\ 2(n_1 + 1 \leq c \leq n_1 + n_2) \\ \vdots \\ t_m(\sum_{i=1}^{t_m-1} n_i + 1 \leq c \leq \sum_{i=2}^{t_m} n_i) \end{cases} \quad \dots (13)$$

つぎに、上記(1)～(4)の分割処理を、具体例を挙げて説明する。例とし

て、AG (2, 2³) の c = 16 番目の列の「1」の行番号を $G_{16} = \{10\ 16\ 18\ 2\ 3\ 35\ 38\ 39\ 49\}$ と定義する。第6図は、ランダム系列のラテン方陣行列による分割手順を示す図である。図示のラテン方陣行列 $L_{j_0}(i)$ の結果を用いて手順 (5) を実行すると、新しい列 $g_{16,e}$ の中の「1」は (14) 式のように表すことができる。

$$g_{16,1}'(1) = g_{16}'(L_{2,8}(1)) = g_{16}'(3) = 18$$

$$g_{16,1}'(2) = g_{16}'(L_{2,8}(2)) = g_{16}'(2) = 16$$

$$g_{16,2}'(1) = g_{16}'(L_{2,8}(3)) = g_{16}'(8) = 49$$

$$g_{16,2}'(2) = g_{16}'(L_{2,8}(4)) = g_{16}'(7) = 39$$

$$10 \quad g_{16,3}'(1) = g_{16}'(L_{2,8}(5)) = g_{16}'(6) = 38$$

$$g_{16,3}'(2) = g_{16}'(L_{2,8}(6)) = g_{16}'(1) = 10$$

$$g_{16,4}'(1) = g_{16}'(L_{2,8}(7)) = g_{16}'(4) = 23$$

$$g_{16,4}'(2) = g_{16}'(L_{2,8}(8)) = g_{16}'(5) = 35 \quad \cdots (14)$$

その結果、16番目の列は以下のように分割される。

$$15 \quad G_{16,1} = \{18\ 16\}$$

$$G_{16,2} = \{49\ 39\}$$

$$G_{16,3} = \{38\ 10\}$$

$$G_{16,4} = \{23\ 35\}$$

このように、本実施の形態では、上記有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法(第2図、ステップS1)を実行することによって、確定的で特性が安定した「Irregular-LDPC符号」用の検査行列 $H(n \times k)$ を生成することができる。

上記のように、パリティ検査行列 H 、生成行列 G 、 G^{-1} ($G^{-1} \cdot G = I$: 単位行列) を生成後、つぎに、送信側の通信装置では、乱数発生部11が、乱数列 (1, 0の列: 送信データ) を発生し、さらに送信コード (+ : 水平垂直方向に偏光された光を識別可能な測定器に対応したコード, × : 斜め方向に偏光された光を識別可能な測定器に対応したコード) をランダムに決定する (ステップS2)。

一方、受信側の装置では、乱数発生部 31 が、受信コード（+：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（ステップ S 12）。

- 5 つぎに、送信側の通信装置では、光子生成部 12 が、上記乱数列と送信コードの組み合わせで自動的に決まる偏光方向で光子を送信する（ステップ S 3）。たとえば、0 と + の組み合わせで水平方向に偏光された光を、1 と + の組み合わせで垂直方向に偏光された光を、0 と × の組み合わせで 45° 方向に偏光された光を、1 と × の組み合わせで 135° 方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

光子生成部 12 により生成した光信号を受け取った受信側の通信装置の光子受信部 32 では、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって自動的に決まる受信データを得る（ステップ S 13）。ここでは、受信データとして、水平方向に偏光された光と + の組み合わせで 0 を、垂直方向に偏光された光と + の組み合わせで 1 を、 45° 方向に偏光された光と × の組み合わせで 0 を、 135° 方向に偏光された光と × の組み合わせで 0 を、それぞれ得る。

- 20 つぎに、受信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べるために、乱数発生部 31 が、受信コードを、公開通信路を介して送信側の通信装置に対して送信する（ステップ S 13）。受信コードを受け取った送信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信側の通信装置に対して送信する（ステップ S 3）。そして、受信側の通信装置および送信側の通信装置では、正しい測定器で受信した受信信号に対応するデータだけを残し、その他を捨てる（ステップ S 3, S 13）。その後、残ったデータをメモリ等に保存し、その先頭から順に n ビットを読み出し、送信データ m_A と受信データ m_B (m_B は伝送路上で雑音等の影響を受けた m_A) を生成する。すなわち、ここでは、共有鍵生成処理が終わる

度につきの n ビットを読み出し、その都度、送信データ m_A と受信データ m_B を生成する。本実施の形態では、正しい測定器で受信した受信信号に対応するビットの位置が、送信側の通信装置と受信側の通信装置との間で共有できている。

つぎに、送信側の通信装置では、シンドローム生成部 1 4 が、パリティ検査行列 H ($n \times k$) と送信データ m_A を用いて m_A のシンドローム $S_A = Hm_A$ を計算し、その結果を、公開通信路通信部 1 3、公開通信路を介して受信側の通信装置に通知する (ステップ S 4)。この段階で、 m_A のシンドローム S_A (k ビット分の情報) は盗聴者に知られる可能性がある。一方、受信側の通信装置では、公開通信路通信部 3 4 にて m_A のシンドローム S_A を受信し、それをシンドローム復号部 3 3 に通知する (ステップ S 1 4)。

シンドローム復号部 3 3 では、パリティ検査行列 H と受信データ m_B を用いて m_B のシンドローム $S_B = Hm_B$ を計算し、さらに、 m_A のシンドローム S_A と m_B のシンドローム S_B を用いてシンドローム $S = S_A + S_B$ を計算する (ステップ S 1 5)。そして、シンドローム S に基づいて送信データ m_A を推定する (ステップ S 1 6)。ここでは、 $m_B = m_A + e$ (雑音等) と仮定し、式 (1 5) に示すようにシンドローム S を変形した後、シンドローム復号により e を求め、送信データ m_A を求める (ステップ S 1 6)。なお、 $S_A + S_B$, $m_A + e$ の $+$ は排他的論理和を表す。

$$\begin{aligned}
 S &= S_A + S_B \\
 &= Hm_A + Hm_B \\
 &= H(m_A + m_B) \\
 &= H(m_A + m_A + e) \\
 &= He \quad \dots (1 5)
 \end{aligned}$$

最後に、受信側の通信装置では、共有鍵生成部 3 5 が、公開された誤り訂正情報 (盗聴された可能性のある上記 k ビット分の情報: S_A) に応じて共有情報 (m_A) の一部を捨てて、 $n - k$ ビット分の情報量を備えた暗号鍵 r を生成する (ステップ S 1 7)。すなわち、共有鍵生成部 3 5 では、先に計算しておいた G^{-1}

($n \times (n - k)$) を用いて下記 (16) 式により暗号鍵 r を生成する。受信側の通信装置は、この暗号鍵 r を送信側の通信装置との共有鍵とする。

$$r = G^{-1}m_A \quad \dots (16)$$

一方、送信側の通信装置においても、共有鍵生成部 15 が、公開された誤り訂正情報（盗聴された可能性のある上記 k ビット分の情報： S_A ）に応じて共有情報（ m_A ）の一部を捨てて、 $n - k$ ビット分の情報量を備えた暗号鍵 r を生成する（ステップ S5）。すなわち、共有鍵生成部 15 では、先に計算しておいた $G^{-1} (n \times (n - k))$ を用いて上記 (16) 式により暗号鍵 r を生成する（ステップ S5）。送信側の通信装置は、この暗号鍵 r を受信側の通信装置との共有鍵とする。

このように、本実施の形態においては、確定的で特性が安定した「Irregular-LDPC符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てる構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。

なお、本実施の形態では、 $HG = 0$ を満たす生成行列 $G ((n - k) \times n)$ から、 $G^{-1} \cdot G = I$ （単位行列）となる逆行列 $G^{-1} (n \times (n - k))$ を生成し、当該逆行列 G^{-1} を用いて共有情報（ n ）の一部（ k ）を捨てて、 $n - k$ ビット分の情報量を備えた暗号鍵 r を生成することとしたが、これに限らず、共有情報（ n ）の一部を捨てて、 m （ $m \leq n - k$ ）ビット分の情報量を備えた暗号鍵 r を生成することとしてもよい。具体的にいうと、 n 次元ベクトルを m 次元ベクトルに写す写像 $F(\cdot)$ を想定する。 $F(\cdot)$ は、共有鍵の安全性を保証するために、「任意の m 次元ベクトル v に対して、写像 F と生成行列 G の合成写像 $F \cdot G$ における逆像 $(F \cdot G)^{-1}(v)$ の元の個数が v によらず一定（ 2^{n-k-m} ）である」、と

いう条件を満たす必要がある。このとき、共有鍵 r は、 $r = F(m_A)$ となる。

実施の形態 2.

実施の形態 2 では、前述した実施の形態 1 における暗号鍵の秘匿性をさらに増強させる。

5 第 7 図は、本発明にかかる量子暗号システムの実施の形態 2 の構成を示す図である。なお、先に説明した実施の形態 1 と同様の構成については、同一の符号を付してその説明を省略する。量子通信路で盗聴された情報に対して秘匿性を増強させるためには、盗聴されたビット数分をハッシュ関数により圧縮する必要がある。しかしながら、ハッシュ関数は、その特性により盗聴されやすい位置が存在
10 する。そこで、本実施の形態においては、その位置をランダムに並べ替えることによって対応する。

第 8 図は、実施の形態 2 の量子鍵配送を示すフローチャートであり、詳細には、送信側の通信装置の処理を示す。送信側の通信装置のランダム置換部 16 では、正則なランダム行列 $R((n-k) \times (n-k))$ を生成し、当該 R を共有鍵生成部 15 に通知し、さらに、当該 R を、公開通信路を介して受信側の通信装置の共有鍵生成部 35 に通知する（ステップ S6）。なお、第 7 図および第 8 図では、
15 一例として、送信側の通信装置でランダム行列 R を生成／送信しているが、これに限らず、この処理は、受信側の通信装置で行うこととしてもよい。

その後、送信側の通信装置では、共有鍵生成部 15 が、公開された誤り訂正情報（盗聴された可能性のある上記 k ビット分の情報： S_A ）に応じて共有情報（ m_A ）の一部を捨てて、さらに、受け取ったランダム行列 R を用いて秘匿性を増強して、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する（ステップ S5）。すなわち、共有鍵生成部 15 では、先に計算しておいた $G^{-1}(n \times (n-k))$ と受け取ったランダム行列 $R((n-k) \times (n-k))$ を用いて下記（17）
25 式により暗号鍵 r を生成する。送信側の通信装置は、この暗号鍵 r を受信側の通信装置との共有鍵とする。

$$r = R G^{-1} m_A \quad \cdots (17)$$

一方、受信側の通信装置においても、共有鍵生成部 35 が、公開された誤り訂正情報（盗聴された可能性のある上記 k ビット分の情報： S_A ）に応じて共有情報（ m_A ）の一部を捨てて、さらに、受け取ったランダム行列 R を用いて秘匿性を増強して、 $n - k$ ビット分の情報量を備えた暗号鍵 r を生成する（ステップ S 17）。すなわち、共有鍵生成部 15 では、先に計算しておいた G^{-1} （ $n \times (n - k)$ ）と受け取ったランダム行列 R （ $(n - k) \times (n - k)$ ）を用いて上記（17）式により暗号鍵 r を生成する（ステップ S 17）。受信側の通信装置は、この暗号鍵 r を送信側の通信装置との共有鍵とする。

このように、本実施の形態においては、確定的で特性が安定した「Irregular-LDPC 符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てて、さらに正則なランダム行列を用いて共有情報を並べ替える構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。さらに、正則なランダム行列を用いて共有情報を並べ替えることとしたため、秘匿性を増強させることができる。

なお、本実施の形態においても、実施の形態 1 と同様に、共有情報（ n ）の一部を捨てて、 m （ $m \leq n - k$ ）ビット分の情報量を備えた暗号鍵 r を生成することとしてもよい。この場合、共有鍵 r は、 $r = RF(m_A)$ となる。

実施の形態 3.

先に説明した実施の形態 1 では、生成行列 G^{-1} を用いて共有情報の一部を捨てていた。これに対して、実施の形態 3 では、生成行列 G^{-1} を用いずに、パリティ検査行列 H の特性を用いて共有情報の一部を捨てる。なお、本実施の形態の構成は、先に説明した実施の形態 1 の第 1 図と同様である。

以下、実施の形態 3 の量子鍵配送について説明する。ここでは、先に説明した

第2図と異なる処理についてのみ説明する。

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部10、30が、特定の線形符号のパリティ検査行列 H ($n \times k$) を求める (ステップS1, ステップS11)。なお、有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法 (第2図ステップS1の詳細) については、先に説明した実施の形態1の第3図と同様である。

そして、実施の形態1と同様の手順でステップS2～S4を実行後、受信側の通信装置では、共有鍵生成部35が、公開された誤り訂正情報 (盗聴された可能性のある上記 k ビット分の情報: S_A) に応じて共有情報 (m_A) の一部を捨てて、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する (ステップS17)。具体的には、共有鍵生成部35が、上記ステップS11で生成したパリティ検査行列の列に対してランダム置換を行う。そして、送信側の通信装置との間で捨てるビットに関する情報を、公開通信路を介して交換する。ここでは、元の有限アフィン幾何 $AG(2, 2^q)$ の1列目の中から特定の「1」を選び、その位置を、公開通信路を介して交換する。

その後、共有鍵生成部35では、上記置換後のパリティ検査行列から上記「1」に対応する分割後の位置、および巡回シフトされた各列における上記「1」に対応する分割後の位置を特定し、その特定した位置に対応する共有情報 m_A 内のビットを捨てて、残りのデータを暗号鍵 r とする。受信側の通信装置は、この暗号鍵 r を送信側の通信装置との共有鍵とする。

一方、送信側の通信装置においても、共有鍵生成部15が、公開された誤り訂正情報 (盗聴された可能性のある上記 k ビット分の情報: S_A) に応じて共有情報 (m_A) の一部を捨てて、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する (ステップS5)。具体的には、共有鍵生成部15が、上記ステップS1で生成したパリティ検査行列の列に対して上記と同様のランダム置換を行う。そして、上記捨てるビットに関する情報を、公開通信路を介して交換する。

その後、共有鍵生成部15では、上記置換後のパリティ検査行列から上記「1

」に対応する分割後の位置、および巡回シフトされた各列における上記「1」に対応する分割後の位置を特定し、その特定した位置に対応する共有情報 m_A 内のビットを捨てて、残りのデータを暗号鍵 r とする。送信側の通信装置は、この暗号鍵 r を受信側の通信装置との共有鍵とする。

- 5 このように、本実施の形態においては、生成行列 G^{-1} を用いずに、パリティ検査行列 H の特性を用いて共有情報の一部を捨てる構成とした。これにより、実施の形態1と同様の効果が得られるとともに、さらに、複雑な生成行列 G 、 G^{-1} の演算処理を削除することができる。

- 10 なお、本実施の形態においては、パリティ検査行列 H の特性を用いて共有情報の一部を捨てて、さらに、実施の形態2と同様に、正則なランダム行列を用いて共有情報を並べ替える構成としてもよい。これにより、秘匿性を増強させることができる。

- 15 以上、説明したとおり、本発明によれば、確定的で特性が安定した「Irregular-LDPC符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる、という効果を奏する。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる、という効果を奏する。
- 20

産業上の利用可能性

- 25 以上のように、本発明にかかる量子鍵配送方法および通信装置は、通信媒体として光子を用いた量子暗号システムに有用であり、特に、高度に安全性の保証された共通鍵を生成するための装置として適している。

請 求 の 範 囲

1. 光子を量子通信路上に送信する第1の通信装置と当該光子を測定する第2の通信装置で構成された量子暗号システムにおける量子鍵配送方法において、

- 5 前記第1および第2の通信装置が、同一のパリティ検査行列 H ($n \times k$) を生成する検査行列生成ステップと、

前記第1の通信装置が、乱数列(送信データ)を発生し、さらに所定の送信コード(基底)をランダムに決定し、前記第2の通信装置が、所定の受信コード(基底)をランダムに決定する乱数発生ステップと、

- 10 前記第1の通信装置が、前記送信データと送信コードの組み合わせによって規定された量子状態で、光子を量子通信路上に送信する光子送信ステップと、

前記第2の通信装置が、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを得る光子受信ステップと、

- 15 前記第1および第2の通信装置が、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定された n ビットの受信データおよび対応する送信データを残し、その他を捨てるデータ削除ステップと、

前記第1の通信装置が、前記パリティ検査行列 H と n ビットの送信データに基づく k ビットの誤り訂正情報を、公開通信路を介して前記第2の通信装置に通知する誤り訂正情報通知ステップと、

- 20 前記第2の通信装置が、前記パリティ検査行列 H と n ビットの受信データと誤り訂正情報に基づいて、受信データの誤りを訂正する誤り訂正ステップと、

前記第1および第2の通信装置が、公開された誤り訂正情報に応じて誤り訂正後の共有情報(n)の一部(k)を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を装置間の共有鍵とする暗号鍵生成ステップと、

- 25 を含むことを特徴とする量子鍵配送方法。

2. 前記検査行列生成ステップにあつては、

基本行列として有限アフィン幾何を用い、ガウス近似法による最適化を行うことによって、パリティ検査行列の最適な行と列の重み配分を探索する重み探索ステップと、

- 5 前記最適な重み配分に基づいて、前記有限アフィン幾何の行および列の重みを所定の手順でランダムに分割し、列と行の重みまたはどちらか一方が均一でない低密度パリティ検査符号のパリティ検査行列Hを生成する分割ステップと、
を含むことを特徴とする請求の範囲第1項に記載の量子鍵配送方法。

- 10 3. 前記検査行列生成ステップにあつては、さらに、「 $HG=0$ 」を満たす生成行列G ($(n-k) \times n$) から、 $G^{-1} \cdot G = I$ (単位行列) となる逆行列 G^{-1} ($n \times (n-k)$) を生成し、

前記暗号鍵生成ステップにあつては、逆行列 G^{-1} を用いて共有情報(n)の一部(k)を捨てることを特徴とする請求の範囲第1項に記載の量子鍵配送方法。

- 15 4. 前記暗号鍵生成ステップにあつては、前記共有情報(n)の一部(k)を捨てた後、一方の装置が、正則なランダム行列R ($(n-k) \times (n-k)$) を生成し、公開通信路を介して他方の通信装置に通知し、前記第1および第2の通信装置が、それぞれ前記ランダム行列Rを暗号鍵に作用させることを特徴とする請求の範囲第3項に記載の量子鍵配送方法。

20

5. 前記検査行列生成ステップにあつては、さらに、n次元ベクトルをm ($m \leq n-k$) 次元ベクトルに写す写像Fで、任意のm次元ベクトルvに対して、写像Fと「 $HG=0$ 」を満たす生成行列Gの合成写像 $F \cdot G$ における逆像($F \cdot G$) $^{-1}(v)$ の元の個数がvによらず一定(2^{n-k-m})であるものを生成し、

- 25 前記暗号鍵生成ステップにあつては、写像Fを用いて共有情報(n)の一部を捨てることを特徴とする請求の範囲第1項に記載の量子鍵配送方法。

6. 前記暗号鍵生成ステップにあつては、前記共有情報 (n) の一部 (k) を捨てた後、一方の装置が、正則なランダム行列 $R ((n-k) \times (n-k))$ を生成し、公開通信路を介して他方の通信装置に通知し、前記第 1 および第 2 の通信装置が、それぞれ前記ランダム行列 R を暗号鍵に作用させることを特徴とする請求の範囲第 5 項に記載の量子鍵配送方法。

7. 前記暗号鍵生成ステップにあつては、前記パリティ検査行列 H の列に対してランダム置換を実行し、前記パリティ検査行列 H の生成元の有限アフィン幾何 $AG(2, 2^s)$ の 1 列目の中から特定の「1」を選び、その位置を、公開通信路を介して交換し、前記置換後のパリティ検査行列から前記「1」に対応する分割後の位置 (列)、および巡回シフトされた各列における前記「1」に対応する分割後の位置 (列)、を特定し、その特定した位置 (列) に対応する共有情報 (n) の一部 (k) を捨てることを特徴とする請求の範囲第 2 項に記載の量子鍵配送方法。

8. 前記暗号鍵生成ステップにあつては、前記共有情報 (n) の一部 (k) を捨てた後、一方の装置が、正則なランダム行列 $R ((n-k) \times (n-k))$ を生成し、公開通信路を介して他方の通信装置に通知し、前記第 1 および第 2 の通信装置が、それぞれ前記ランダム行列 R を暗号鍵に作用させることを特徴とする請求の範囲第 7 項に記載の量子鍵配送方法。

9. 光子を量子通信路上に送信する通信装置において、
受信側の通信装置と同一のパリティ検査行列 $H (n \times k)$ を生成する検査行列生成手段と、
乱数列 (送信データ) を発生し、所定の送信コード (基底) をランダムに決定し、当該送信データと送信コードの組み合わせによって規定された量子状態で光子を量子通信路上に送信し、その後、前記受信側の通信装置における測定が正し

い測定器で行われたものかどうかを調べ、正しい測定器で測定された n ビットの送信データを残し、その他を捨てる送信手段と、

前記パリティ検査行列 H と n ビットの送信データに基づく k ビットの誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知する誤り訂正情報通知手段と、

公開した誤り訂正情報に応じて誤り訂正後の共有情報 (n) の一部 (k) を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を受信側の通信装置との共有鍵とする暗号鍵生成手段と、

を備えることを特徴とする通信装置。

10

10. 前記検査行列生成手段は、

基本行列として有限アフィン幾何を用い、ガウス近似法による最適化を行うことによって、パリティ検査行列の最適な行と列の重み配分を探索し、

前記最適な重み配分に基づいて、前記有限アフィン幾何の行および列の重みを所定の手順でランダムに分割し、

列と行の重みまたはどちらか一方が均一でない低密度パリティ検査符号のパリティ検査行列 H を生成することを特徴とする請求の範囲第9項に記載の通信装置。

11. 前記検査行列生成手段は、さらに、「 $HG = 0$ 」を満たす生成行列 G ($(n-k) \times n$) から、 $G^{-1} \cdot G = I$ (単位行列) となる逆行列 G^{-1} ($n \times (n-k)$) を生成し、

前記暗号鍵生成手段は、逆行列 G^{-1} を用いて共有情報 (n) の一部 (k) を捨てることを特徴とする請求の範囲第9項に記載の通信装置。

12. 前記暗号鍵生成手段は、前記共有情報 (n) の一部 (k) を捨てた後、正則なランダム行列 R ($(n-k) \times (n-k)$) を前記暗号鍵に作用させることを特徴とする請求の範囲第11項に記載の通信装置。

25

- 1 3. 前記検査行列生成手段は、さらに、 n 次元ベクトルを m ($m \leq n - k$)
次元ベクトルに写す写像 F で、任意の m 次元ベクトル v に対して、写像 F と「 H
 $G = 0$ 」を満たす生成行列 G の合成写像 $F \cdot G$ における逆像 $(F \cdot G)^{-1}(v)$
5 の元の個数が v によらず一定 (2^{n-k-m}) であるものを生成し、

前記暗号鍵生成手段は、写像 F を用いて共有情報 (n) の一部を捨てることを
特徴とする請求の範囲第9項に記載の通信装置。

- 1 4. 前記暗号鍵生成手段は、前記共有情報 (n) の一部 (k) を捨てた後、
10 正則なランダム行列 R ($(n - k) \times (n - k)$) を前記暗号鍵に作用させるこ
とを特徴とする請求の範囲第13項に記載の通信装置。

- 1 5. 前記暗号鍵生成手段にあつては、前記パリティ検査行列 H の列に対して
ランダム置換を実行し、前記パリティ検査行列 H の生成元の有限アフィン幾何 A
15 $G(2, 2^s)$ の1列目の中から特定の「1」を選び、その位置を、公開通信路
を介して交換し、前記置換後のパリティ検査行列から前記「1」に対応する分割
後の位置 (列)、および巡回シフトされた各列における前記「1」に対応する分
割後の位置 (列)、を特定し、その特定した位置 (列) に対応する共有情報 (n
) の一部 (k) を捨てることを特徴とする請求の範囲第10項に記載の通信装置。

20

- 1 6. 前記暗号鍵生成手段は、前記共有情報 (n) の一部 (k) を捨てた後、
正則なランダム行列 R ($(n - k) \times (n - k)$) を前記暗号鍵に作用させるこ
とを特徴とする請求の範囲第15項に記載の通信装置。

- 25 1 7. 量子通信路上の光子を測定する通信装置において、

送信側の通信装置と同一のパリティ検査行列 H ($n \times k$) を生成する検査行列
生成手段と、

所定の受信コード（基底）をランダムに決定し、量子通信路上の光子を測定し、前記受信コードと測定結果の組み合わせによって規定された受信データを再生し、その後、前記測定が正しい測定器で行われたものかどうかを調べ、正しい測定器で測定された n ビットの受信データを残し、その他を捨てる受信手段と、

- 5 公開通信路を介して受信した k ビットの誤り訂正情報と、前記パリティ検査行列 H と n ビットの受信データと、に基づいて、受信データの誤りを訂正する誤り訂正手段と、

- 10 公開された誤り訂正情報に応じて誤り訂正後の共有情報（ n ）の一部（ k ）を捨てて、残りの情報で暗号鍵を生成し、この暗号鍵を送信側の通信装置との共有鍵とする暗号鍵生成手段と、

を備えることを特徴とする通信装置。

18. 前記検査行列生成手段は、

- 15 基本行列として有限アフィン幾何を用い、ガウス近似法による最適化を行うことによって、パリティ検査行列の最適な行と列の重み配分を探索し、

前記最適な重み配分に基づいて、前記有限アフィン幾何の行および列の重みを所定の手順でランダムに分割し、

- 20 列と行の重みまたはどちらか一方が均一でない低密度パリティ検査符号のパリティ検査行列 H を生成することを特徴とする請求の範囲第17項に記載の通信装置。

19. 前記検査行列生成手段は、さらに、「 $HG=0$ 」を満たす生成行列 G （ $(n-k) \times n$ ）から、 $G^{-1} \cdot G = I$ （単位行列）となる逆行列 G^{-1} （ $n \times (n-k)$ ）を生成し、

- 25 前記暗号鍵生成手段は、逆行列 G^{-1} を用いて共有情報（ n ）の一部（ k ）を捨てることを特徴とする請求の範囲第17項に記載の通信装置。

20. 前記暗号鍵生成手段は、前記共有情報 (n) の一部 (k) を捨てた後、正則なランダム行列 $R ((n-k) \times (n-k))$ を前記暗号鍵に作用させることを特徴とする請求の範囲第19項に記載の通信装置。

5 21. 前記検査行列生成手段は、さらに、 n 次元ベクトルを m ($m \leq n-k$) 次元ベクトルに写す写像 F で、任意の m 次元ベクトル v に対して、写像 F と「 $HG=0$ 」を満たす生成行列 G の合成写像 $F \cdot G$ における逆像 $(F \cdot G)^{-1}(v)$ の元の個数が v によらず一定 (2^{n-k-m}) であるものを生成し、

10 前記暗号鍵生成手段は、写像 F を用いて共有情報 (n) の一部を捨てることを特徴とする請求の範囲第17項に記載の通信装置。

22. 前記暗号鍵生成手段は、前記共有情報 (n) の一部 (k) を捨てた後、正則なランダム行列 $R ((n-k) \times (n-k))$ を前記暗号鍵に作用させることを特徴とする請求の範囲第21項に記載の通信装置。

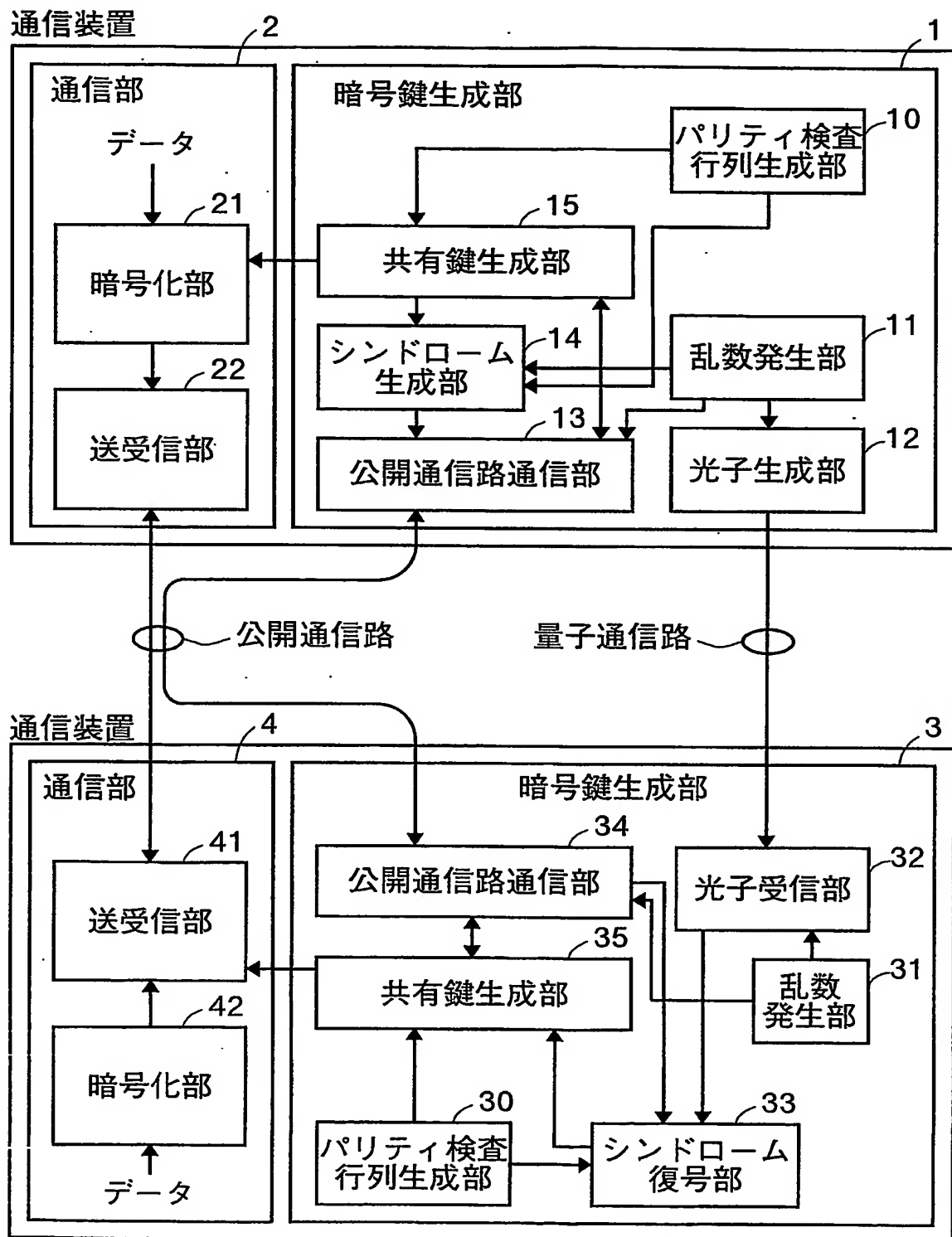
15

23. 前記暗号鍵生成手段にあつては、前記パリティ検査行列 H の列に対してランダム置換を実行し、前記パリティ検査行列 H の生成元の有限アフィン幾何 $AG(2, 2^s)$ の1列目の中から特定の「1」を選び、その位置を、公開通信路を介して交換し、前記置換後のパリティ検査行列から前記「1」に対応する分割後の位置 (列)、および巡回シフトされた各列における前記「1」に対応する分割後の位置 (列)、を特定し、その特定した位置 (列) に対応する共有情報 (n) の一部 (k) を捨てることを特徴とする請求の範囲第18項に記載の通信装置。

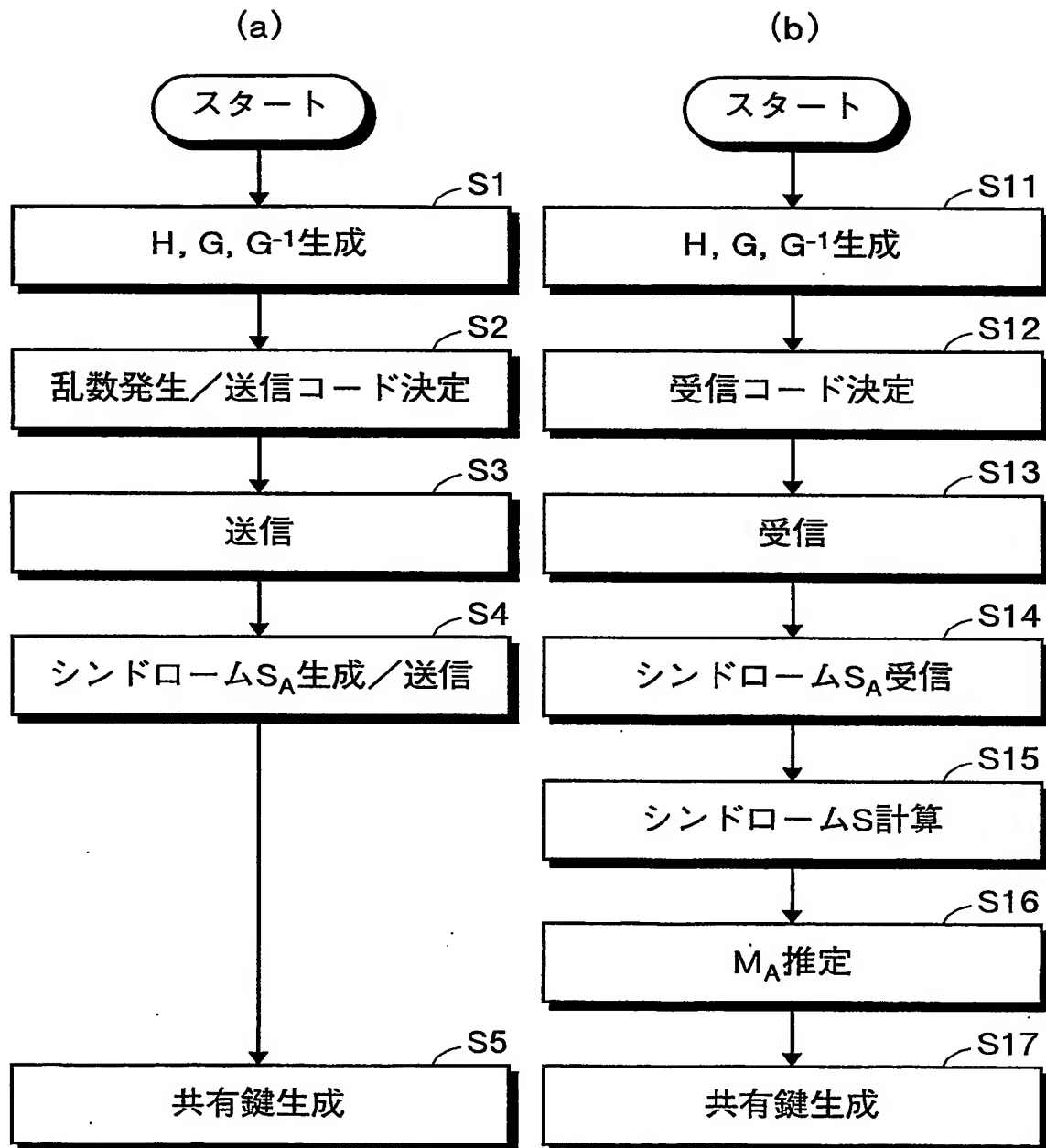
20

24. 前記暗号鍵生成手段は、前記共有情報 (n) の一部 (k) を捨てた後、
25 正則なランダム行列 $R ((n-k) \times (n-k))$ を前記暗号鍵に作用させることを特徴とする請求の範囲第23項に記載の通信装置。

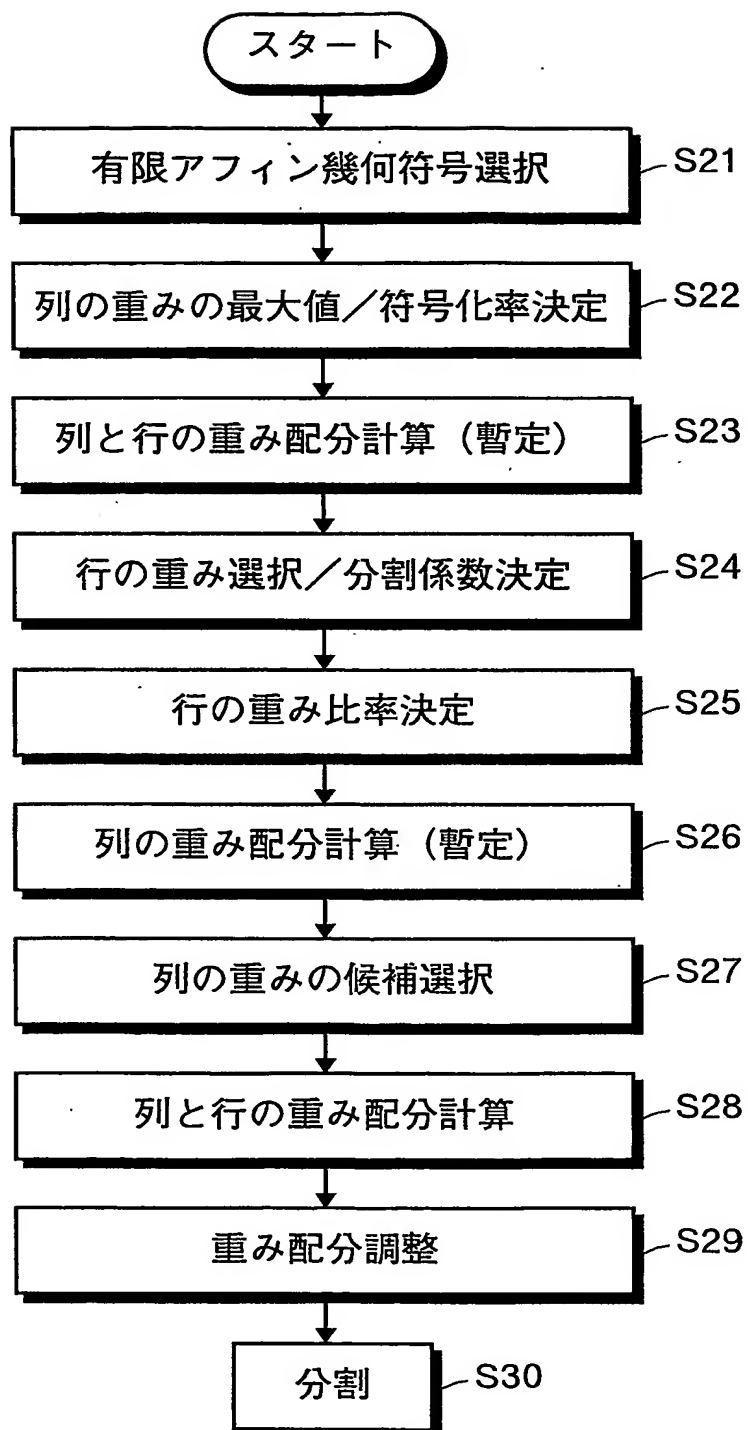
第1図



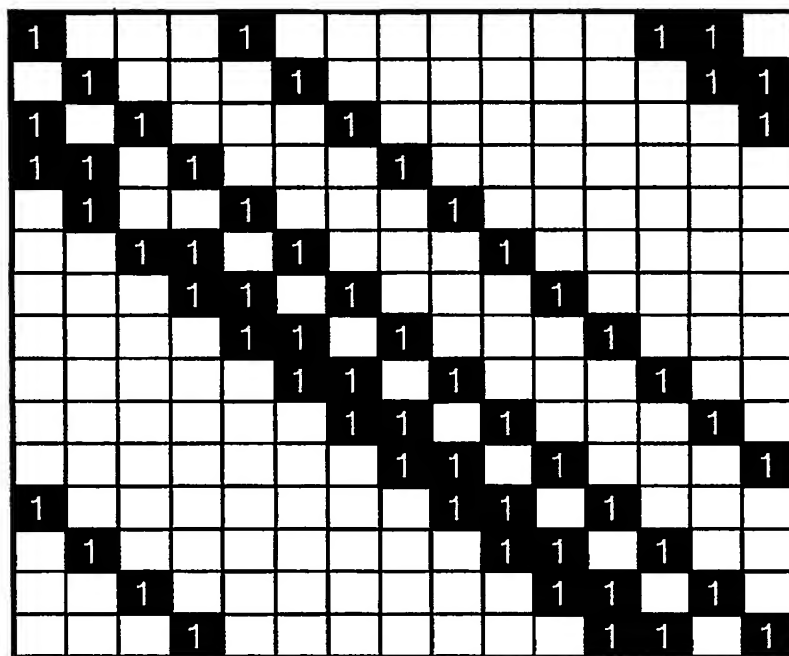
第2図



第3図



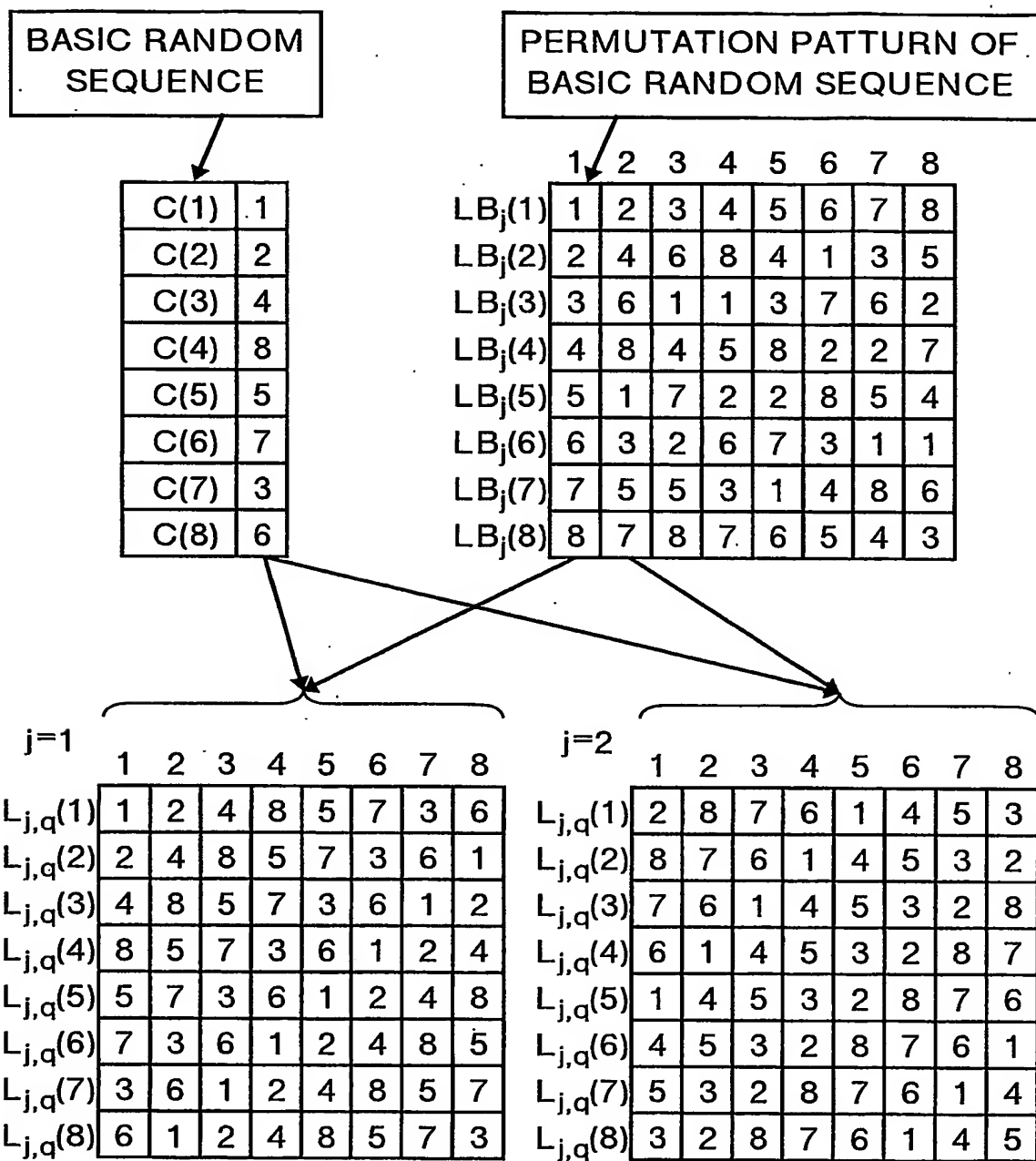
第4図



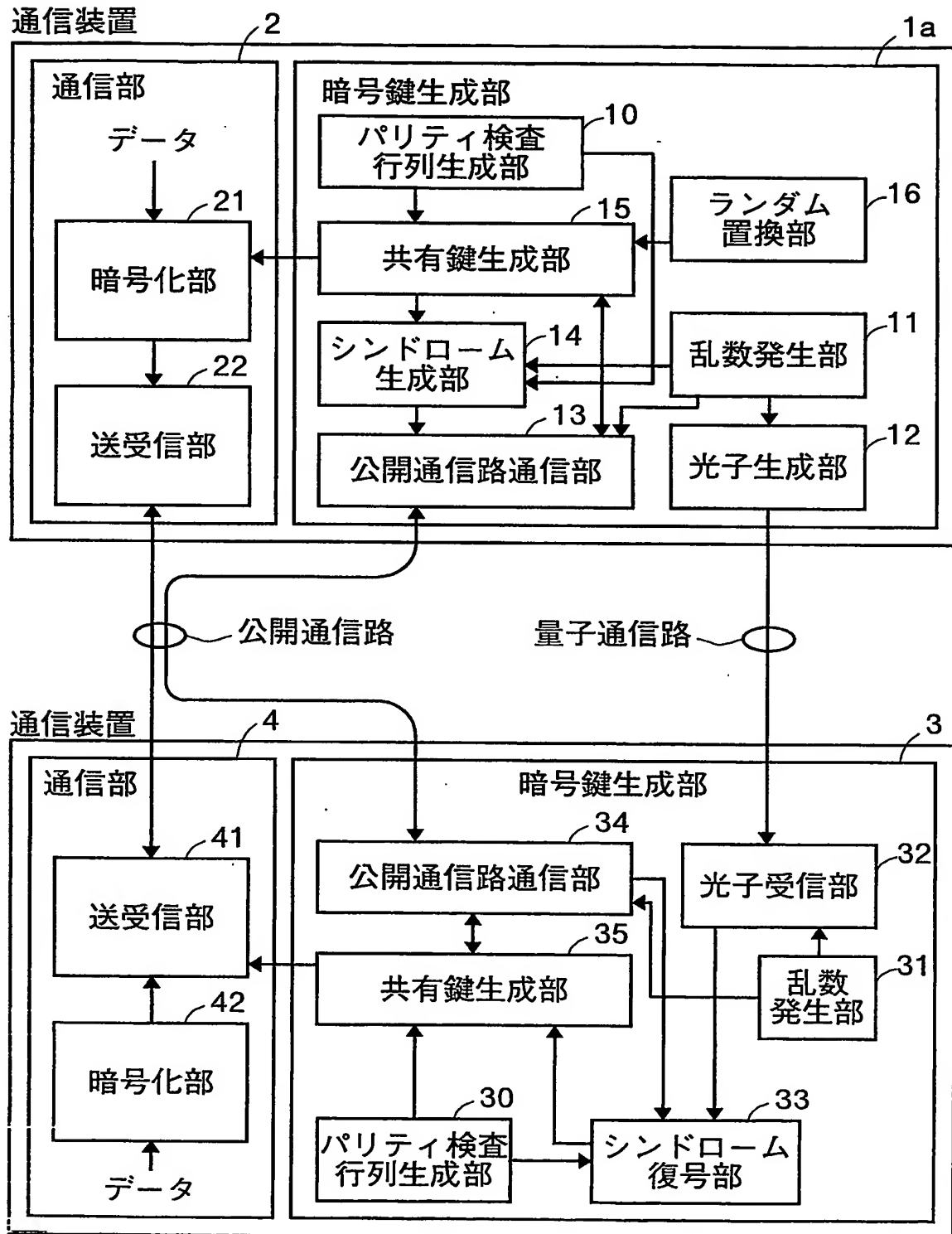
第5図

rate		0.5	
N		12.6	
i	γ_i	$\lambda(\gamma_i)$	$n(\gamma_i)$
1	2	0.27381	69
2	3	0.10714	18
3	8	0.61905	39
u		ρ_u	nu
8		1	63

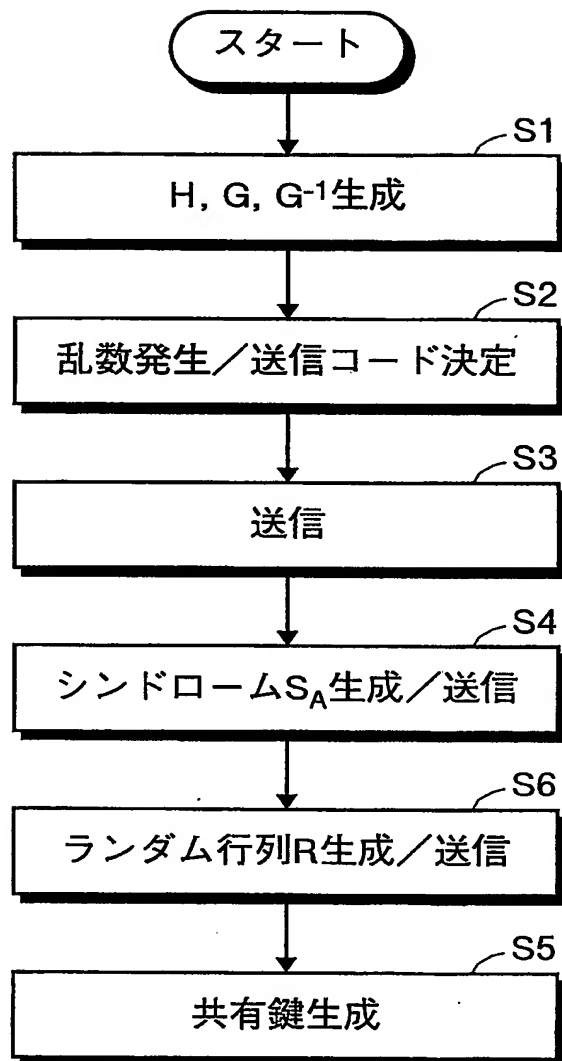
第6図



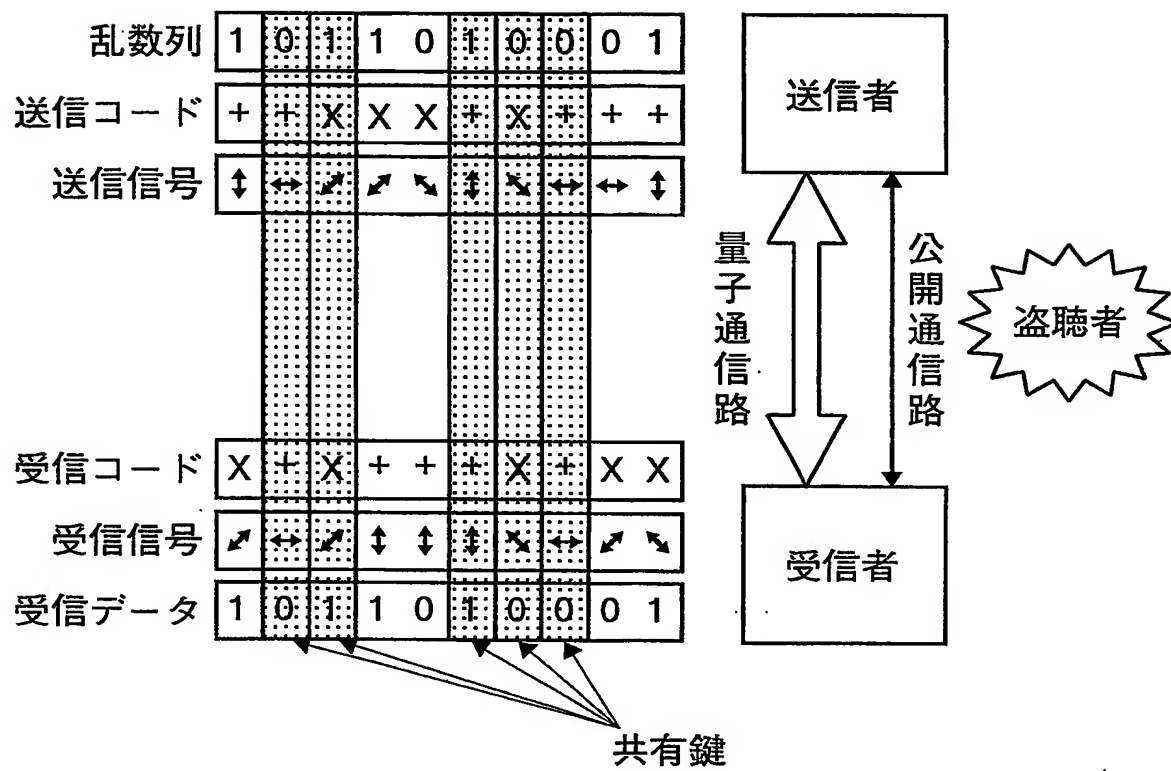
第7図



第8図



第9図



INTERNATIONAL SEARCH REPORT

National application No.

PCT/JP03/11706

A. CLASSIFICATION OF SUBJECT MATTER Int.Cl ⁷ H04L9/12, H03M13/09, H04B10/00										
According to International Patent Classification (IPC) or to both national classification and IPC										
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int.Cl ⁷ H04L9/12, H03M13/09, H04B10/00										
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched <table style="width: 100%; border: none;"> <tr> <td style="width: 33%;">Jitsuyo Shinan Koho</td> <td style="width: 33%;">1922-1996</td> <td style="width: 33%;">Toroku Jitsuyo Shinan Koho</td> <td style="width: 33%;">1994-2003</td> </tr> <tr> <td>Kokai Jitsuyo Shinan Koho</td> <td>1971-2003</td> <td>Jitsuyo Shinan Toroku Koho</td> <td>1996-2003</td> </tr> </table>			Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003	Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003
Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003							
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003							
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)										
C. DOCUMENTS CONSIDERED TO BE RELEVANT										
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.								
Y	Rikako UCHIYAMA, "Ryoshi Rikigaku no Kiso to Ryoshi Ango Ryoshi Tsushin Channel no Shiten", Suuri Kagaku No.12, Vol.34, No.12, 01 December, 1996 (01.12.96), pages 53 to 61	1-24								
Y	Koichi YAMAZAKI, "Ryoshi Ango Kagi Haisokei no Tame no Ayamari Teisei Fugo", 2001 Nen The Institute of Electronics, Information and Communication Engineers Sogo Taikai Koen Ronbunshu, Kiso-Kyokai, 07 March, 2001 (07.03.01), pages 556 to 557	1-24								
Y	Yu Kou and Shu Lin, Marc P.C. Fossorier: "Low Density Parity Check Codes: Construction Based on Finite Geometries", 2000 IEEE GLOBECOM, received on 31 January, 2001 (31.01.01), pages 825 to 829	2,7,8,10,15, 16,18,23,24								
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.										
*	Special categories of cited documents:									
"A"	document defining the general state of the art which is not considered to be of particular relevance									
"E"	earlier document but published on or after the international filing date									
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)									
"O"	document referring to an oral disclosure, use, exhibition or other means									
"P"	document published prior to the international filing date but later than the priority date claimed									
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention									
"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone									
"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art									
"&"	document member of the same patent family									
Date of the actual completion of the international search	Date of mailing of the international search report									
16 December, 2003 (16.12.03)	13 January, 2004 (13.01.04)									
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer									
Facsimile No.	Telephone No.									

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/11706

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Sae-Young Chung, Thomas J. Richardson, and Rudiger L. Urbanke: "Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation", IEEE TRANSACTIONS ON INFORMATION THEORY, Vol.47, No.2, received on 09 April, 2001 (09.04.01), pages 657 to 670	2, 7, 8, 10, 15, 16, 18, 23, 24
A	Akihiro YAMAMURA, Yuichi ISHIZUKA, "Ryoshi Ango Tsushin ni okeru Ayamari Kenchi to Privacy Amplification", 2001 Nen Ango to Joho Security Symposium Yokoshu, Vol.1 of 2, 23 January, 2001 (23.01.01), pages 73 to 78	1-24

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/12 H03M13/09 H04B10/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/12 H03M13/09 H04B10/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2003年
日本国登録実用新案公報	1994-2003年
日本国実用新案登録公報	1996-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	内山智香子: “量子力学の基礎と量子暗号 量子通信チャンネルの視点”, 数理科学 12号, 第34巻12号, 1996. 12. 01, p. 53-61	1-24
Y	山崎浩一: “量子暗号鍵配送系のための誤り訂正符号”, 2001年電子情報通信学会総合大会講演論文集, 基礎・境界, 2001. 03. 07, p. 556-557	1-24

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

16. 12. 03

国際調査報告の発送日

13.01.04

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳



5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	Yu Kou and Shu Lin , Marc P.C. Fossorier: "Low Density Parity Check Codes:Construction Based on Finite Geometries" , 2000 IEEE GLOBECOM, 2001. 01. 31受入, p. 825-829	2, 7, 8, 10, 15, 16, 18, 23, 24
Y	Sae-Young Chung, Thomas J. Richardson, and Rudiger L. Urbanke : "Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation" , IEEE TRANSACTIONS ON INFORMATION THEORY, VOLUME 47, NUMBER 2, 2001. 04. 09受入, p. 657-670	2, 7, 8, 10, 15, 16, 18, 23, 24
A	山村明弘, 石塚裕一: "量子暗号通信における誤り検知とプライバシーアンプリフィケーション", 2001年暗号と情報セキュリティシンポジウム予稿集, Volume 1 of 2, 2001. 01. 23, p. 73-78	1-24